Pairing-based Cryptography: Identity Based Encryption and Beyond

Dustin Moody
NIST
What is Pairing-based Cryptography?

• Tool for building public key primitives
  – new features
  – improved efficiency for some protocols
  – uses different mathematical structure

• First papers published in 2001
  – identity-based encryption (Boneh, Franklin)
  – short signatures (Boneh, Lynn, Shacham)
Identity-based Encryption (IBE)

• Concept: Shamir 1984
  – No scheme though

• Basic idea
  – Public key can be an identifier (e.g. email address)
  – A private key generator (PKG) generates per user private key

• Distinctive property
  – A sender can send encrypted messages before the recipient obtains his private key.
Emerging Technologies

• Short signatures
• Attribute-based encryption
  – Allows only people with certain attributes the ability to decrypt messages
• Functional encryption
  – uses pairings to construct decryption keys that map ciphertext to an arbitrary function of the plaintext.
• Searchable encryption
  – allows searching an encrypted database without having to decrypt the database
• (ID-based) signcryption, hierarchical encryption, threshold schemes, aggregate signatures, chameleon hashes, blind signatures, group signatures,…
Pairings in Standards

• Pairings in the standards
  – IEEE P1363.3
  – IETF S/MIME
  – X9F1 (proposal)
  – ISO
  – TCG (proposal)
Call for Feedback

• In 2008, NIST held a workshop on pairing-based cryptography

• NIST is currently studying pairing based schemes to better understand their security, possible applications, etc.

• We would like feedback on use cases for pairing-based cryptography. This will help us grasp the practical demand and impact of this new technology: pairings@nist.gov